Cyber Intel Advisory:
Boston Marathon Bombing Is Being Used to Disseminate Malware and Conduct Financial Fraud

16 April 2013

Integrated Intelligence Center
Multi-State Information Sharing and Analysis Center
William F. Pelgrin, President and CEO

The Risk: The bombing of the Boston Marathon, 15 April 2013, does not just mean an increased threat level across the country and globe, but includes new and recycled Internet scams. Major events tend to attract malicious individuals who use the event for their gain.

The Threats: Internet watch groups and cyber security experts have already identified multiple fake domains/websites, and charity efforts taking advantage of the Boston Marathon bombing. Based on previous tragedies, more scams will follow in the coming days. Internet users need to apply a critical eye and conduct due diligence before clicking links, visiting websites, or making donations.

- Actors with unknown intentions registered over 125 domain names associated with the Boston Marathon bombings and victims, in the hours after the incident. The majority of these new domains use a combination of the words "Boston," "Marathon," "2013," "bomb," "explosions," "attack," "victims," and "donate" and should be viewed with caution. More domains are likely to follow.
- Malicious actors are using social networking websites to spread hoaxes, including information regarding the purported death of several child runners (children are not allowed to participate in the Boston Marathon), and injured runners purportedly running for a variety of charities and causes.
- Phishing emails may provide links to malicious websites purporting to contain information, pictures, and video, or may contain attachments with embedded malware. Clicking on the links or opening the attachments can infect the victim's computer to further malicious activity.
- Multiple fake charities were created on social networking websites within minutes of the explosions purporting to collect funds for victims. Traditionally, these websites are scams.

The Action: Users should adhere to the following guidelines when reacting to large news events, including news associated with the Boston Marathon bombing, and solicitations for donations:

- Be cautious of emails/websites that claim to provide information because they may contain viruses.
- Do not open unsolicited (spam) emails, or click on the links/attachments contained in those messages.
- Never reveal personal or financial information in email.
- Do not go to untrusted or unfamiliar websites to view the event or information regarding it.
- Never send sensitive information over the Internet before checking a website's security and confirming its legitimacy. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net)

The information provided above is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. Organizations have permission and are encouraged to brand and redistribute this advisory in whole for educational, non-commercial purposes. For more information regarding potential cyber threats please visit the Center for Internet Security website at CISecurity.org.